第1章 設計品質確保の思想

── 航空宇宙エレクトロニクスに学ぶ「信頼性設計」

檜原弘樹

航空機や宇宙機に搭載する機器のエレクトロニクス設計では，高い信頼性が要求されます．そのため，部品・材料の信頼性，工程の信頼性，機器（デバイス）の信頼性，そしてシステムの信頼性を階層的に保証しながら製品開発を進めています．本稿ではその一例として，人工衛星のエレクトロニクス設計においてどのように信頼性保証がなされているのかを概観します．こうした考えかたは，ディジタル家電や車載機器といった民生用機器の開発とも共通します．（筆者）

ユビキタス社会は「どこでもコンピュータ環境」とも言われます(1)．すでに，高性能なマイコンが組み込まれたさまざまな電子機器がいたるところに偏在（ubiquitous）するようになりました（**図1**）．身の回りにあって触れることのできる家電機器から，ふだんはなかなか目に触れないところで着実に稼働している制御装置まで，さまざまな組み込み機器に囲まれて，私たちは日々生活しています．

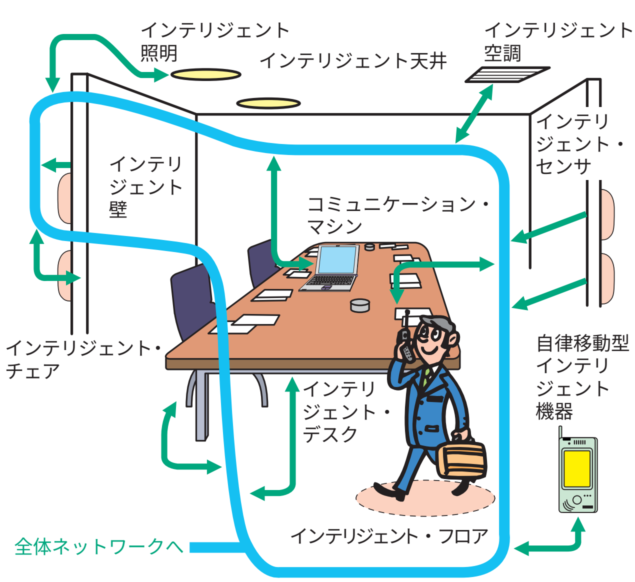


図1　トロンプロジェクトが考える「どこでもコンピュータ環境」
「どこでもコンピュータ環境」とは，身の回りのあらゆる機器，設備，道具にマイクロコンピュータが組み込まれ，それらがネットワークを介して相互に通信し，協調動作することによって，人間の活動を多様な側面から支援する，高度にコンピュータ化された社会環境である．本図は，社団法人トロン協会に提供していただいた図をもとに作成した．

その中でも人工衛星や航空機は，距離的にもっとも離れた場所にある巨大な組み込み機器といえます．先日引退して新型機にバトンタッチした気象衛星「ひまわり5号」（**図2(a)**）は，地球から36,000km離れた静止軌道注1で設計寿命を大幅に上回る8年間にわたって雲画像の取得を行い，天気の予報に役立ってきました．さらには，世界初の小惑星への着陸を果たし，試料採取を試みた「はやぶさ」（**図2(b)**）のように，高度に自律動作する人工衛星もあります．この人工衛星は，地球から3億kmも離れた場所で，搭載したカメラや距離を測るレーザを用いて，みずからの判断で小惑星Itokawaを追走しました．

これらの人工衛星のうち，地表から数百kmの上空を回っているものはスペース・シャトルなどを利用して人手で修理できる場合もありますが，ほとんどのものはいったん打ち上げたら外から修理できません．それなのに，ロケットで打ち上げられる際には10G～20G注2の振動レベルに耐え，宇宙空間に放出された後は大きな温度差や強い放射線にさらされます（**図3**）．

さらに，人工衛星の打ち上げは以前より低コスト化が進んでいるものの，数十億～100億円以上の費用がかかります．その投資がむだにならないように，着実にミッションをこなせるだけの高信頼性を有するシステムを開発する必

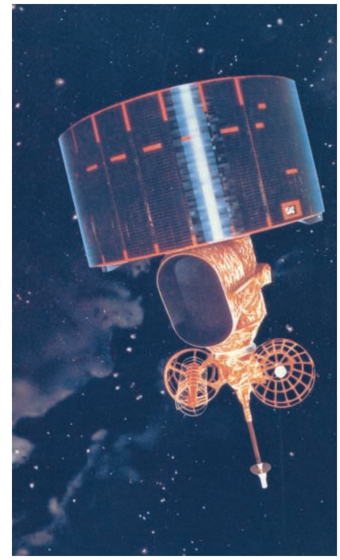
注1：地表面からあたかも止まっているように見える速度で人工衛星が地球の周りを回る軌道．
注2：ちなみに，戦闘機では最大9Gくらいの重力がかかることがある．これは70kgの人が突然630kgの体重になることに相当する．

図2
人工衛星の外観(想像図)

(a)のひまわり5号は，1995年3月18日にH-IIロケット3号機によって打ち上げられた静止気象衛星．高度36,000kmの静止軌道に位置し，可視・赤外センサにより雲の分布などの撮像を行う．2003年5月22日に観測を米国の「ゴーズ9号(パシフィックゴーズ，東経155°)」に引き継いだ．質量は345kg．(b)のはやぶさは，2003年5月9日にM-Vロケット5号機によって打ち上げられた工学実験探査機．電気推進エンジンとスイングバイ技術により，はるか3億kmかなたの小惑星Itokawaへ到達した．そして，航法用カメラとレーザ高度計を用いてみずから判断して推進エンジンを調節し，小惑星Itokawaへの降下を行った．2005年11月26日にItokawa上のミューゼスの海付近に着陸し，試料の採取を試みた．



(b) はやぶさ



(a) ひまわり5号

提供：宇宙航空研究開発機構(JAXA)

要があります．

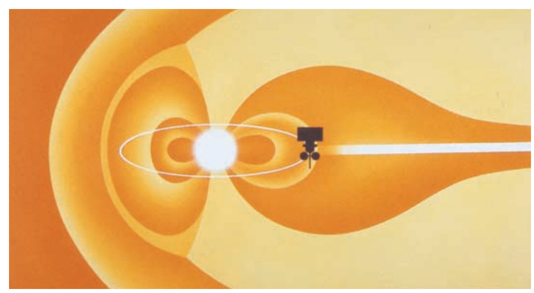
このような環境に対応するため，信頼性の高い設計手法が整備されつつありますが，その高い信頼性は，「部品の選択」や「ハードウェア設計」，「ソフトウェア設計」，「システム設計」といった種々のレベルの設計を着実に積み上げて初めて達成されるものです．つまり，特殊な設計手法が使われているわけではなく，また，用いられている技術の多くも，ディジタル家電や車載機器などの民生用機器の開発手法と同じです(p.42のコラム「民生用機器と宇宙機器の接点」を参照)．

1 人工衛星に見る信頼性設計の考えかた

以下では，人工衛星のような高信頼性システムの設計プロセスを概観するとともに，随所で民生用機器の信頼性設計に通じるところがある点を紹介します．

● 無線やデータ処理，カメラ，制御，電源などを統合

人工衛星は，地上(地球上)の運用設備から遠隔制御によって操作します．無線通信によりコマンド(指令)を送出し，折り返し無線電波に乗って返ってくる各種の状態を示す信号(テレメトリ)を解析して，その人工衛星がどのような状態にあるのかを把握します．搭載されたカメラで撮像された画像データや，衛星回線を用いて伝送される通信データなども，並行して電波で送られてきます．したがって，搭載しているアンテナやカメラがつねに一定の方向に向くように，人工衛星は姿勢や軌道をみずから制御しています．ほとんどの人工衛星は動作に要する電力を太陽電池によって得ているため，太陽電池がつねに太陽の方向を向くように自律的に機体を制御する必要があります．



提供：宇宙航空研究開発機構(JAXA)

図3 放射線にさらされる人工衛星(想像図)

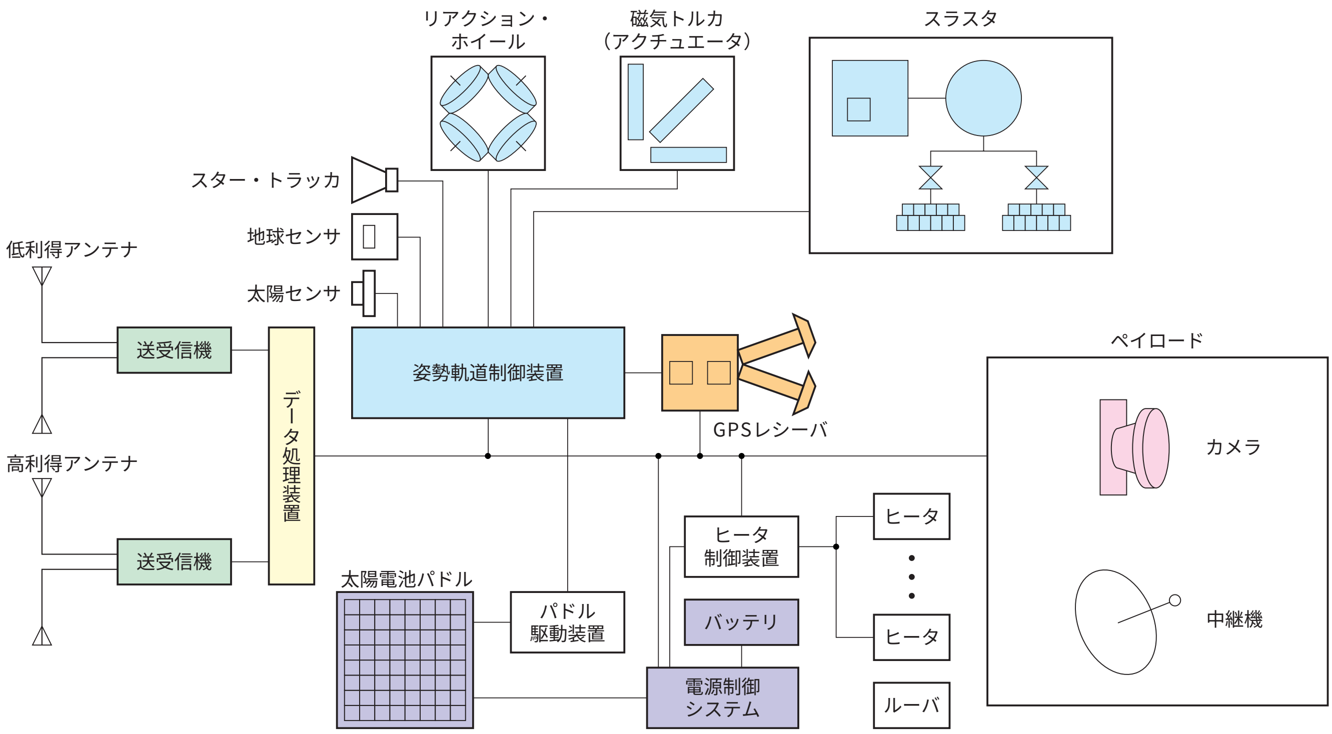
大気にさえぎられることのない宇宙空間では，銀河宇宙線や地球の磁場に補足されたエネルギーの高い放射線が高濃度で存在する．そのため，人工衛星に使用されている部品を保護するためのさまざまの対策が施されている．近年，LSIの微細化とともに，地上の微量な放射線でもソフト・エラーが起こるようになり，宇宙システム機器で用いられている放射線対策と同じソフト・エラー対策が民生機器でも用いられるようになってきた．

さらに近年の人工衛星は，地上局の運用担当者の負担を極力減らすように，「自動化」，「自律化」といった機能を備えています．すなわち，あらかじめ決められた運用シーケンスに従って処理を進めます(自動化)．そして，地上局に送信するテレメトリを自身でもモニタし，緊急の場合には消費電力を絞るなどの緊急退避モードに移行します(自律化)．

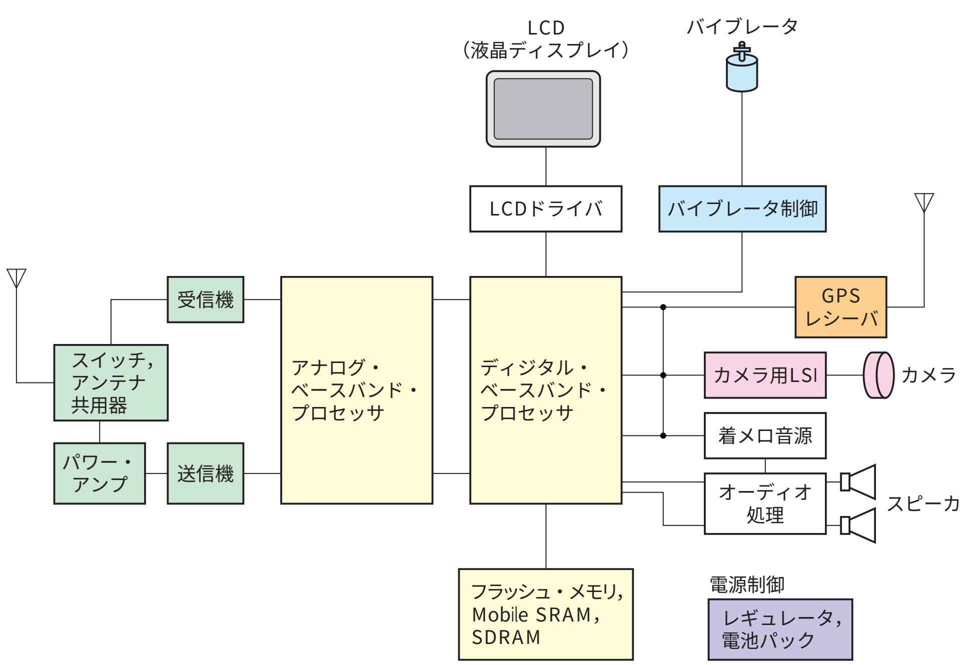
このほかにもペイロード，ないしはミッション機器と呼ばれるカメラや通信機など，人工衛星に搭載されている機器を制御しながら，地球上の人々の生活を支えるさまざまな情報を提供しています．

図4(a)に，簡略化した人工衛星のブロック図を示します．

コマンドやテレメトリは，低利得アンテナを介して送受



(a) 人工衛星



(b) 携帯電話

図4
人工衛星と携帯電話の機能ブロック図

(a)は,簡略化した人工衛星の機能を示している.地上からの無線通信により遠隔制御されるとともに,自動化・自律化によってみずから運用制御を行う機能も有している.このため,組み込みマイコンが多用されるようになってきている.(b)は,携帯電話の模式的な機能を示している.電源制御機能やバイブレータによる着信通知機能などを備えており,自律的に動作するようになっている.また,近年の高機能化に伴い,カメラやGPSレシーバなどが内蔵されるようになった.外形は小さいが,規模は大きな組み込み機器となっている.

信されます.このアンテナは40kbps程度と伝送速度は遅いのですが,広い指向性を有しているので,人工衛星の姿勢が多少傾いても通信リンクを維持できるようになっています.一方,画像データや衛星通信に使用される信号は,高利得アンテナを用いて伝送されます.このアンテナは指向性が強いので,確実に決まった方向を向くように制御する必要があります.

データ処理装置は,地上運用設備から受信したり,みずから自動的に発生したコマンドを人工衛星内の各機器に送出します.そして,それらの機器のテレメトリを収集し,

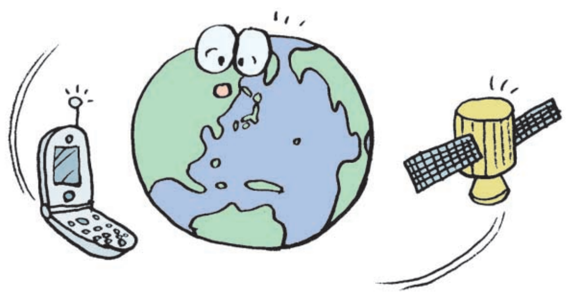


図5　人工衛星は宇宙を駆ける携帯電話!?

人工衛星と携帯電話の機能構成は，驚くほど似通ったものとなってきている．これは，無線通信機器という共通の特徴に加えて，近年の高機能化により，携帯電話に自律的な動作や種々のデータ取得機能が追加されるようになったためである．

表1　人工衛星と携帯電話の機能対比

機能カテゴリ	人工衛星	携帯電話
無線通信	アンテナ，送受信機	アンテナ，送受信機
コンピュータ	データ処理装置	アナログ/ディジタル・ベースバンド・プロセッサ
カメラ	カメラ，観測センサ	カメラ
位置認識	GPSレシーバ，観測センサ	GPSレシーバ
メカトロニクス	姿勢軌道制御装置	バイブレータ制御
電力制御システム	太陽電池パドル，バッテリ，電力制御装置，電力安定化装置	電池パック，レギュレータ
熱制御システム	ルーバ，ヒータ	最適な放熱設計

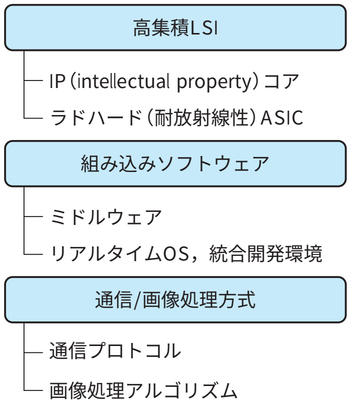


図6　人工衛星と携帯電話の技術要素

高集積LSI，組み込みソフトウェア，通信/画像処理方式からなる．人工衛星と携帯電話は，機能構成だけでなく，実装時の技術要素も共通している．

一定のフォーマットに従って編集し，地上運用設備に送信します．

姿勢軌道制御装置は，搭載している各種のセンサからデータを収集し，それらのデータをもとにアクチュエータを制御して，姿勢や軌道を一定に保ちます．センサには，地球を見てだいたいの姿勢を判断する「地球センサ」，太陽の強い光を見て中程度の精度で姿勢を判断できる「太陽センサ」，多くの星を見て高精度で姿勢や軌道を判断できる「スター・トラッカ（恒星センサ）」，そして近年多くの自動車にも装備されており，高精度で位置を検出できる「GPS（global positioning system）レシーバ」などがあります．アクチュエータには，コマの原理を応用して姿勢を制御する「リアクション・ホイール」，天体が持つ微弱な磁気を利用して姿勢を制御する「磁気トルカ」，燃料を噴射して大きく姿勢や軌道を変える「スラスタ」などがあります．

電源制御システムは，太陽電池パドルによって発電された電力を安定的に各機器に供給しつつ，バッテリに蓄える制御を行います．

人工衛星は激しい寒暖のある宇宙空間にさらされています．そこで熱制御システムが，熱制御材（断熱材など）やルーバ（放熱制御板），ヒータをうまく活用して，人工衛星の内部を0℃～20℃程度に保つように制御しています．

このように，人工衛星は無線通信，コンピュータ，カメラ，メカトロニクス，電力制御システム，熱制御システム，推進系システムなどが統合された，大規模な組み込み機器であるといえます．

● 人工衛星は宇宙を駆ける“携帯電話”!?

ところで，この人工衛星の機能構成は，実は一般の民生用機器と大きく変わるものではありません．

一例として，図4(b)に一般的な携帯電話のブロック図を示します．携帯電話には，通話回線用アンテナ，送受信機，ベースバンド・プロセッサ，カメラ，バイブレータ制御，電池パック，レギュレータなどがあり，これは人工衛星の機能ブロック図とよく似ています（図5）．各機能の対応を表1に示します．

また，人工衛星に使われている実装時の技術要素も，一般の民生用機器とほぼ同じものです（図6）．一部，ラドハード（耐放射線性）LSIなどが使われていますが，高集積LSIはディジタル家電や車載機器でも必須の部品です．人工衛星は，基本ソフトウェアとしてリアルタイムOSを用いており，ソフトウェアの統合開発環境が重要となってきています（ディジタル家電はもとより，最近では自動車のエンジン制御などにもリアルタイムOSが採用されている）．データ圧縮を含む画像処理技術や通信プロトコル技術も，とくに異なるところはありません．

これらのよく知られた技術を用いて，数百km～数億kmのかなたで厳しい環境にさらされながら，修理を期待せず

ミッションを達成する機器を，着実にていねいに実現していくのが人工衛星の開発です．もちろん，ひとりのエンジニアだけでこのような開発を完遂できるわけはありません．さまざまな視点を有するメンバがチームを組み，クロスチェックやレビューを繰り返しながら，非修理系である宇宙システム機器の信頼性を保証します．

● 人工衛星の開発プロセスはウォータ・フォール型

人工衛星の開発プロセスは，いわゆる伝統的なウォータ・フォール型（各工程が完了すると，前の工程へ逆戻りせず，1方向に工程を進める手法）注3が基本となっています（図7）．まず，地球観測や天文観測，衛星通信などの要求仕様を明確にします．続いて，開発が進む中で仕様変更や部品・材料の調達状況，実施されたテスト（製造検査）工程などを確実に記録し，いつでも再確認できるトレーサビリティ管理が行われます．

人工衛星の開発は国家プロジェクトとして進められることが多かったことから，多くの技術基準が文書化されています．それらを参照しながら，基準に合っていることを確認していきます．そして，一般的な環境における機能・性能テストから，打ち上げ，軌道上の厳しい環境を模擬したテストまでを着実に実施し，出荷します．

人工衛星の開発は，具体的には以下のステップに従って進められています．

1）研究フェーズ

研究フェーズでは，人工衛星が用いられるミッションの内容についてユーザとの調整を進め，開発仕様としてミッション要求を設定します．これらは基本仕様や開発計画としてまとめられ，全体的な開発方針が設定されます．

また，この研究フェーズでは，開発する人工衛星がどのようなものになるべきかを決める概念設計が行われます．ここでは最終的に衛星が伝送するデータを利用するユーザや運用担当者との調整を繰り返し，衛星が持つべきミッション要求を明らかにしていきます．この過程で基本仕様，およびどのような開発方針で進めるのかを設定し，開発計画をまとめます．また，新規の技術要素として何があるのかを調査し，新たに研究開発が必要と判断されたもの（例えば，新しい部品など）については開発対象として選考します．

2）開発研究フェーズ

開発研究フェーズは予備設計とも呼ばれます．ここでは開発する人工衛星の仕様や開発計画を詳細化し，文書化します．また，開発計画を遂行することのできる開発体制もこのフェーズで確立されます．

並行して進められる新規技術要素の研究開発については，この予備設計のフェーズで試作テストが行われ，開発を進められるめどが立たなくてはなりません．この段階で作られる試作機をBBM（breadboard model）と呼びます．このフェーズで所定の機能や性能が得られることを確認したら，その後，信頼性保証を行うための工程を確立することになります．

3）開発フェーズ

開発仕様，開発計画，開発体制が整備され，新規技術要素の試作テストが成功すると，いよいよ人工衛星の開発が始まります．この開発フェーズは，大きく四つの工程に分けて管理されています．

「基本設計」の工程では，エンジニアリング・モデルやプロトタイプ・モデルの設計を行います．各種の解析を実施

注3：この開発手法をNASAではPPP（Phased Project Planning）と称して取り入れている．

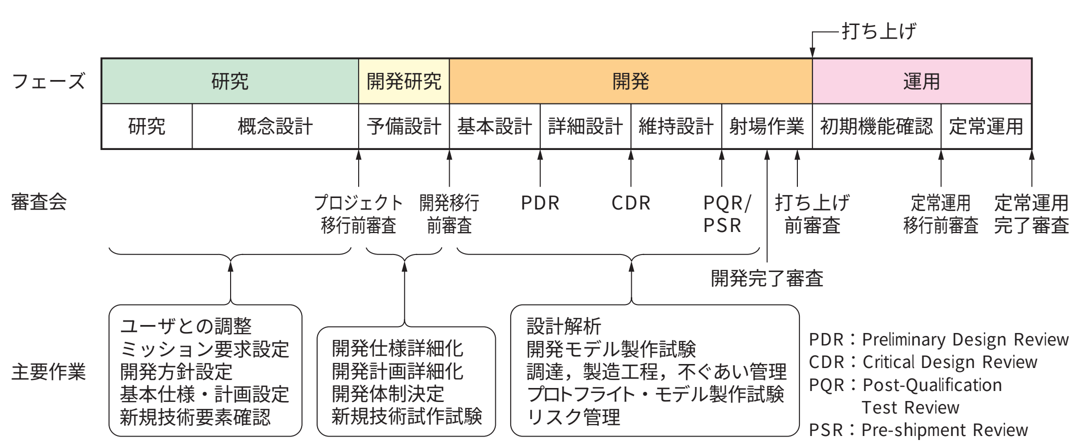


図7 人工衛星開発の流れ
人工衛星は，全体としては地上運用設備も含めた大規模なシステムであり，典型的なウォータ・フォール・モデルに従って開発される．近年，組み込みマイコンを多用するようになり，個々のコンポーネント単位ではさまざまな開発プロセス（開発手法）が導入・評価されている．

し，所定の機能・性能を達成できることを確認します．また，厳しい宇宙環境で所定の期間，運用可能なことを確認します．これらの設計解析結果をもって基本設計審査会（PDR：Preliminary Design Review）を開催し，試作品の製造に取りかかってよいかどうかを審査します．

「詳細設計」の工程では，装置の試作を通じて最終的な設計を確定します．また，実際に厳しい宇宙環境を模擬したテストを行い，製造プロセスとテスト・プロセスを確立します．これらの結果を反映し，打ち上げるモデル（フライト・モデル）の設計を進めます．製造テストの結果を評価し，詳細設計資料を審査することにより，フライト品[注4]の製造に取りかかってよいかどうかを審査します．

「維持設計」の工程では，フライト品の製造・テストを進める中で，各種のドキュメントの維持・改訂も含めて製品としてまとめる作業を進め，打ち上げの準備を行います．人工衛星の製造・テストが完了し，打ち上げに向けた文書などの準備が完了すると，品質に関する認定試験後審査（PQR：Post-Qualification Test Review），および出荷前審査（PSR：Pre-Shipment Review）を行います．

この審査をパスすると，人工衛星はロケット発射場へと出荷されます（「射場作業」の工程）．

4）運用フェーズ

運用フェーズでは，打ち上げた直後に軌道上で初期テストを行い，所定の機能や性能が得られていることを確認します．その後，一連の定常運用を実施して，実運用が可能であることを確認します．一連のテストが終わったら最終的なユーザに引き渡され，人工衛星の利用フェーズへと移行します．

● 組み込みソフト開発の管理手法をFPGA開発にも適用

人工衛星のテスト・プロセスについては，技術革新に合わせてさまざまな見直しが図られています．ハードウェアやソフトウェアに対してスパイラルな開発手順（設計・実装を反復的に繰り返しながら完成度を高めていく手法）やアジャイルな手法（顧客の要求や開発プロジェクトの状況の変化に迅速に対応する手法）などが適宜試験的に適用され，評価されています．人工衛星の開発全体では前述のウォータ・フォール型プロセスが維持されていますが，ほかの手法についても良い点は個別に取り入れています．

組み込みマイコンやPLD/FPGAなどの利用が広がるにつれて，設計手法のソフトウェア化が進んでいます．ディスクリート部品やICをプリント基板上で結線していた時代とは異なり，開発の途中で設計を修正しやすくなっています．人工衛星の開発は3年から，長いものでは7年にわたることもあるため，単なる不ぐあいの解消だけでなく，新規技術の取り込みも起こりえます．

組み込みマイコンの導入が進んだころは，不ぐあいの修正部分は組み込みソフトウェアに偏りがちでした．しかし，最近ではFPGAの採用が進み，FPGAの修正で対処することも珍しくなくなってきました．修正しやすいということは，柔軟な開発が可能となる反面，最終的な設計の確定が遅れがちになるというリスクもはらんでいます．そのため，設計プロセスの管理が重要になります．

組み込みソフトウェアの開発規模が大きくなるにつれて，汎用的な機能を備えるミドルウェアやソフトウェア・コンポーネントの導入が進んでいます．信頼性を確保するために再利用の重要性が説かれていますが，実際に再利用を進めていくと，ソフトウェアのインターフェース仕様を容易に変えにくいという問題にぶつかります．こうしたソフトウェアとハードウェアのインターフェース仕様のギャップを埋めるためにFPGAが活用されるケースも増えています．

FPGAの開発では，VHDLやVerilog HDLなどのハードウェア記述言語を使う手法が一般化しています．また，C言語ベースの設計環境も整備され始めたことから，FPGAの設計はますます柔軟になっていくと思われます．このためもあり，筆者らの間では，従来，組み込みソフトウェアに適用されてきたプロジェクト管理の手法がFPGAの設計管理にも適用されるようになっています．従来のハードウェア設計者，ソフトウェア設計者という枠組みを超えた素養を持ち，ハードウェアとソフトウェアの間を線引きしない，柔軟な考えかたを持ったエンジニアがますます必要となっています．

● 信頼性は製品の特性ではなく目標達成のための評価指標

さて，前述のようにステップ・バイ・ステップで工程を進めながら宇宙環境で所定の期間，機能・性能を維持する人工衛星を開発するわけですが，筆者らがどのような観点で信頼性を確保しながら開発を進めているのかを述べます．

工業製品としての信頼性の公式な定義は，JIS-Z-8115に

注4：日本では製造する人工衛星はそれほど多くない．開発した最初のモデルが実際の運用に供せられることが多いため，プロトフライト・モデル（proto-flight model）とも呼ばれる．

述べられているように，「アイテムが，与えられた条件のもとで，規定の期間中，要求された機能を果たせる性質」です．一般的な概念として，狭義には所定の使用環境でいかに故障せず，長持ちできるかという性質になります．広義に解釈すると，上記に加えて，万一故障しても迅速に復旧し，サービスを継続維持できる性質となります．維持・修理などの保全性や可用性（availability）も含むと考えると，信頼性（信頼度）は時間的品質を表す尺度であるとも考えられます．

品質の保証とは，単に製品の質の良さだけを保証するのではなく，製品を生み出すシステム（受注→開発・設計→製造→テスト→保管→輸送→納入のライフ・サイクル）の質の良さも維持・保証することと考えられ，一種の総合品質保証（total quality assurance）であると見なせます．これを人工衛星に当てはめると，「所定のミッション期間中，運用環境下において故障しないこと」，「一部で故障が発生しても全体に影響が波及せず，システム機能を維持してミッションを達成できること」と言い換えられます．

人工衛星そのものは今や技術的にかなり確立された工業製品であり，信頼性保証は「あたりまえの品質」としてとらえられています．また，人工衛星を所定の期間，問題なく運用できて，そのミッションを達成できることが，要求される信頼性といえます．

すなわち信頼性とは，製品そのものの特性ではなく，ミッション達成を保証するための重要な評価指標であるといえます．そして，設計，製造，テスト，運用の全ライフ・サイクルを通じて配慮するべきものなのです．

2 システム全体の信頼性を確保する方法

高信頼性を要求される人工衛星の場合でも，「良い製品は，良いプロセス，良いチームから生まれる」という一般的な原則は同じです．

● 高信頼性システムを実現するための四つのポリシ

高信頼性システムを作り出すにあたっては，以下の四つのポリシを着実に実践していきます．

1）最初から正しく作る

不良要因を埋め込まない要求分析，設計手法，およびプロセスを確立し，維持することが重要です．検証や設計の

Column 1 民生用機器と宇宙機器の接点

人工衛星などの宇宙システムでは，これまで特殊な規格が用いられることが多かったため，テストでは，オシロスコープやロジック・アナライザなどの汎用測定器を除くと，専用の装置が用いられてきました．しかし最近では，RISCプロセッサが搭載されるようになった結果，ICE（in-circuit emulator）やソフトウェアの統合開発環境など，民生用機器の開発と共通のものが使われるようになり，さまざまな技術交流が行われています．

また，宇宙機器向けのインターフェース規格として，IEEE 1355を改良した“SpaceWire”という規格が提唱されています．これは，FPGAとLVDSバッファがあれば数Mbps～数百Mbpsの通信を容易に実現できるインターフェースです．かならずしも専用デバイスを必要としないことから，**写真A-1**に示すような低コストの評価装置が共同開発されています．SpaceWireは非常に低コストで実現できるという特徴を備えています．また，故障時にう回路を簡単に実現でき，一本のケーブルでは伝送容量が足りない場合に動的に複数のケーブルを用いて大容量データを送ることができます．そのため，マルチメディア通信機器や車載機器の関係者からも関心が高く，宇宙航空研究開発機構 宇宙科学研究本部内にSpaceWireユーザー会が発足しています[注A-1]．

注A-1：http://www.isas.jaxa.jp/j/researchers/の「SpaceWireを用いた次世代アーキテクチャ」を参照．



提供：宇宙航空研究開発機構（JAXA）

写真A-1　SpaceCube

SpaceCubeは外形寸法が52mm×55mm×55mmのコンピュータで，T-Engine仕様と互換性のあるT-Engineアプライアンスである．100Mbps以上の通信レートを有するポートを三つ備えている．また，ディスプレイ，キーボード，マウスを接続すると電子プレゼンテーションも可能．EthernetやUSBのポートも備える．これにSpaceWire（宇宙機器向けインターフェース規格）のアナライザが実装されたテスト装置として，販売が予定されている．

妥当性確認，デザイン・レビューを通じて不良を未然に防止するプロセスも，あわせて維持します．漏れのないテストを行うことは重要ですが，予備的に開発されたもの（試作機など）に対してテストで保証できるわけではありません．

2）見逃さない

製品開発では，自社で開発するものばかりではなく，外部から調達するものもあります．埋もれているかもしれない不良要因を確実に洗い出し，顕在化する前に是正するしくみを確立する必要があります．例えば，スクリーニング試験やバーンイン・テストなどの各種テスト，データ分析評価を開発プロセスに組み込みます．テスト方法は網羅性を考慮して体系的に計画します（いわゆるテスト設計）．また，取得されたテスト・データを適宜参照・活用できるように環境を整備する必要があります．

3）リスクに備える

万が一不ぐあいが発生しても，その影響が最小になるように，あらかじめ考えうるリスクを洗い出し，予想して対処するように努力します．

4）コンティンジェンシ（緊急時）に対応する

不ぐあいが発生したら，確実に処置が反映され，そのことが関係部署に通知されるシステムを構築・維持します．例えば，不ぐあい情報を迅速にアラート（警報）として通知する情報伝達のしくみや，品質上の"ヒヤリハット"（ヒヤリとかハッとしたトラブル事例）を埋もれさせない注意体制，教訓を確実に伝承するしくみの構築などが挙げられます．

● システム全体の信頼性は階層的に押さえる

システム全体の信頼性を保証するには，階層的なアプローチで押さえていきます．すなわち，部品・材料の信頼性，工程の信頼性，機器（デバイス）の信頼性，システムの信頼性を着実に積み上げます．各階層ごとに潜在する問題を抽出し，各階層における保証技術を組み合わせて適用します．また，分析や評価に基づく種々の選択肢のトレードオフ評価を行い，設計の最適化を考慮して処置を決定し，製品の製造・テストを通じてその妥当性を確認します．そして，必要に応じて下位の階層に立ち戻り，修正します．さらに，ほかの製品の開発プロジェクトへ修正が必要なことを伝達しなければならない場合もあります．

1）部品・材料の信頼性

人工衛星を開発するにあたって，信頼性の高い部品や材料を選択することはたいせつです．設計や運用のくふうでその欠点を補える場合もありますが，この場合，追加コストが発生したり，運用上のリスクが生じることがあります．

通常は，信頼性の確保が保証されている部品や材料を調達します．使用上の目的に応じて民生部品を用いることもありますが，その場合でも宇宙用部品のテスト手法に基づいた信頼性テストを行います．製造ロットなどの部品の履歴を管理し，ロケットで人工衛星を打ち上げる際の環境や宇宙空間の環境に耐えうるものであるかどうかを確認して使用します（pp.44-45のコラム「宇宙放射線環境下の半導体デバイス」を参照）．

人工衛星に使用する部品の選択については，宇宙空間特有の配慮はあるものの，それ以外は高い信頼性を要求される地上システム向けの部品の場合とあまり差異はありません．さまざまな情報を収集して素材が良い部品を選択し，部品メーカ（自社で部品を製造する場合も含む）が持つ加工・製造技術や完成度を見極めて，安定的に供給できるメーカから部品を調達します．また，工場の製造プロセス（歩留まり，ばらつき）やメーカの検査体制を確認します．もちろん，部品のフィールド実績も重要な情報となります．とくに，FPGAやEEPROM，SRAM，FIFOメモリなど，世代交代の早いデバイスは，十分な情報収集と適合性評価が必要になります．

部品を購入する際には，部品・材料の製造プロセス管理を確認し，スクリーニング試験やロット保証試験，例えば寿命試験や破壊試験（DPA：destructive physical Analysis）などを自社で行ったり，スクリーニングを専門とする会社に委託します．近年のシステムLSI化の進展やマルチチップ・モジュールの動向，高密度実装への移行にともなって，部品の構造に着目した確認も必要となってきています．これらの信頼性を保証する工程の費用がコストの大部分を占め，一般に宇宙システム用部品はとても高価なものとなります．

2）工程の信頼性

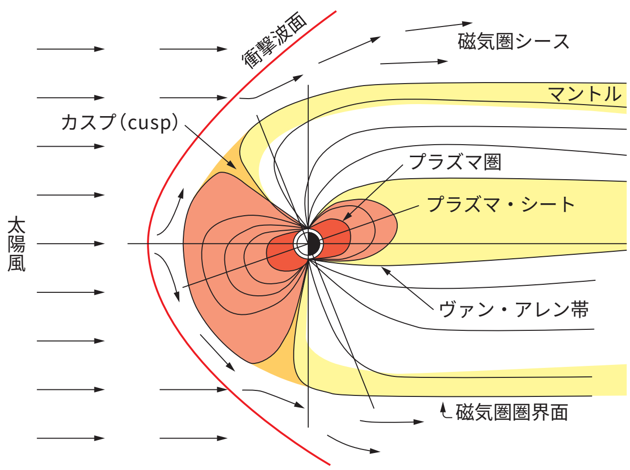
工程の信頼性は，いわゆるノウハウや企業文化が現れるところです．設計過誤防止や検証・検査体制，ヒューマン・ファクタ分析の活用と情報伝達（再発防止対策の徹底），効率化と標準化（検査基準の維持・改訂，自動化推進，治工具改善）など，地道な活動が信頼性を確保する工程を作り上げます．

近年，さまざまな作業が電子化されつつありますが，設計者が製造現場に足を運び，どのように自分の設計したも

Column 2　宇宙放射線環境下の半導体デバイス

ここでは宇宙空間で部品がさらされる環境について紹介します．これらは地球上では通常，経験しない環境ですが，半導体プロセスの微細化に伴って，類似の影響が現れるケースも出てきています[2]．

人工衛星に使用する電子部品は，ロケットで打ち上げる際に激しい振動や温度変化にさらされます．無事打ち上げに成功し，初期の運用準備を経て地球を回る軌道などに安定すると，とくに激しい振動にさらされることはなくなります．温度についても，近年の人工衛星システム設計技術の進歩により，通常は一定の範囲内にコントロールされた環境で運用されるようになっています．



図B-1　宇宙放射線

地球近傍では，太陽風と地球磁気圏に捕捉された放射線が存在する．太陽風は太陽表面から吹き出す約10nT（ナノテスラ）の磁場を伴った超音速のプラズマ（電荷を帯びた粒子）の流れである．地球近傍におけるその速度は約300km/sにも達する．主成分は陽子．そのほか，電子，α粒子，重イオン粒子も存在する．地球磁気圏は宇宙空間の中で地球が持つ磁場の勢力が届く領域である．地球の持つ磁場が太陽風の影響によって太陽方向でつぶれ，夜側に向かって引き延ばされ，捕捉放射線が存在する．

しかし，いったん大気圏から外へ出ると，宇宙空間特有の高い放射線にさらされます．この宇宙放射線環境のもとになるのは宇宙空間に存在する高エネルギー粒子です．これには陽子（プロトン）や電子，中性子，重イオン粒子，α粒子などがあります．なかでも量的に多いのは太陽風（solar wind）が運ぶ放射線です．これらの放射線が地球の磁気圏（magnetosphere）にとらえられているようすを**図B-1**に示します．

この高エネルギー粒子が半導体デバイスに与える影響として，以下のようなものが挙げられます．

1）トータル・ドーズ効果

トータル・ドーズ効果は，部品がさらされる放射線の総量に応じて，半導体デバイスの性能が劣化する現象です．これは永久劣化とみなされ，トランジスタのしきい値が変化することなどにより，性能が劣化していきます．この現象は，主として陽子と電子によって引き起こされるものです．これらの粒子が大量に飛び込んできても，時間がたつと影響が緩和される（アニール効果と呼ばれる）場合もありますが，一般には劣化を抑えるのは難しく，金属などの遮へいによって影響を軽減させる対策が一般的です．

2）シングル・イベント・アップセット

シングル・イベント・アップセット（SEU：single event upset）は，メモリやフリップフロップなどのLSI内の回路に重イオン粒子や

のが製造され，テストされるのかをこまめに確認することが重要です．また，スキルを持つさまざまな分野の作業者と密にコミュニケーションをとることも大事です．

3）機器（デバイス）の信頼性

機器のレベルでは，信頼性を確保するための具体的な機能を設計に組み込みます．例えば回路設計では，冗長回路や故障分離/保護回路を組み込んだり，ストレスのかからない動作条件を設定します．

例えば，上掲のコラム「宇宙放射線環境下の半導体デバイス」で紹介したソフト・エラー対策については，人工衛星では主としてエラー検出・訂正機能の組み込みで対処しています．民生用機器でもソフト・エラー対策設計は同じだと思います．

また，近年の全自動洗濯機は単に一連のシーケンスを実行するだけでなく，洗濯層内の状態をモニタして洗濯物を傷めずに汚れを落とす機能が実装されています．そのため，組み込みマイコンを使って高度な制御を行います．このとき，モータなどのノイズ源と共存して要求機能を達成しなければなりません．そこで，ノイズに起因するメモリのデータ化けでプログラムが暴走するのを防ぐため，定期的にメモリの内容をリフレッシュしています．これなどは，放射線の影響を防ぐために定期的にメモリの内容をリフレッシュする宇宙機器の技術と共通です．また，パソコンやサーバのエラー訂正，およびハード・ディスク装置の読み出し信号のエラー検出/訂正に用いられているリードソロモン符号なども，基本的に人工衛星で用いられているものと共通の技術です．

そのほか，熱・構造設計（熱応力，ひずみ，剛性，強度余裕など），耐環境性設計（熱真空，振動衝撃，放射線，EMCなど），部品のディレーティング解析や回路ストレス解析なども，高信頼性機器を実現するうえで重要な項目です．

さらに，近年は安全性なども重視されるようになってき

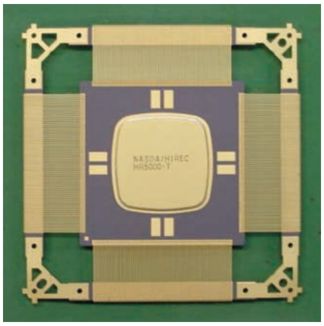
陽子などの高エネルギー粒子が当たり，データが反転してしまう一過性の故障です．一般には「ソフト・エラー」と呼ばれています．いくら正しいソフトウェアやデータがメモリに格納されていても，このような誤りが発生してしまうとマイクロプロセッサなどの誤動作を引き起こします．物理的にデータの反転が起こりにくい半導体デバイスを選択したり，正しいデータをつねにリフレッシュするなどの設計上の対策がとられています．

3）シングル・イベント・ラッチアップ

シングル・イベント・ラッチアップ（SEL：single event latch-up）は，前述のSEUと同じように高エネルギー粒子の放射線によって引き起こされる現象です．一般に，LSIなどの半導体デバイスには回路構成の組み合わせによりサイリスタとよく似た回路ができていることがあります．この半導体基板上に形成されているサイリスタ構造に高エネルギー粒子が当たってしまうと，この部分の回路がONしてしまい，過大な電源電流が流れます．一過性の故障ではなく永久故障につながることがあるので，「ハード・エラー」とも呼ばれます．

上記のSEUとSELを合わせてシングル・イベント効果（SEE：single event effect）と呼びます．このほかにもさまざまな放射線による影響があります．そのため，物理的な観点から放射線に強いデバイスを選択したり，装置設計やシステム設計において，故障が生じてもほかに影響が波及せず，また，できるだけ回復が図れるようなくふうを施します．厳しい宇宙環境に耐え，高い信頼性管理の下で作られている64ビットRISCマイクロプロセッサの例を**写真B-1**に示します．

これらの放射線環境については，従来は宇宙空間特有のものとして扱われていました．しかし，昨今の半導体プロセスの微細化により，デバイスのパッケージから放出される微量の放射線や，地球上の自然放射線によって引き起こされるデータ・エラー（前述のソフト・エラー）が顕在化してきています．このため，宇宙システムの設計技術者が家電機器などの民生用機器の設計技術者と情報交換するケースも出てきています(2)．民生用機器の開発者が半導体プロセスの微細化に伴って直面しているソフト・エラーへの対策は，激しい放射線環境にさらされる宇宙システムの設計技術者が数十年前から実施してきたものと非常に近いものになっています．



提供：宇宙航空研究開発機構（JAXA）

写真B-1　宇宙システム用64ビットRISCマイクロプロセッサ（HR5000）

プロセッサ・コアとして，MIPS 5kfを採用している．過酷な環境で長期間安定して動作するように開発された．UARTやタイマ，DMAコントローラ，割り込みコントローラなどの周辺回路を内蔵している．若干の外付け部品とメモリ・システムを追加することにより，計算機システムを構築できる．メモリ・コントローラは標準でEDAC（error detection and correction）機能を備えている．

ています．人工衛星はロケットで打ち上げることもあり，以前から安全性設計が重視されてきました．民生用機器においても，欧州でIEC 61508などの安全性基準が規格化され，自動車などに取り入れられるようになっています．故障モードを網羅的に拾い上げるFMEA（failure mode effect analysis）や，寿命解析を含むワースト・ケース解析も車載機器の設計などで広く用いられています．

もちろん，このような規格や形式化された手法に基づくチェックばかりでなく，設計部門のノウハウなどを文書化したチェックリストや検証マトリックス，関係者によるデザイン・レビューなどは，宇宙機器の設計に限らず，一般的によく行われており，信頼性を作り込むうえで重要な要素となっています．

4）システムの信頼性

システムの信頼性を決定する要因は，機器の開発/稼働実績，システム・エンジニアリング，プロジェクト管理などです．機器を組み合わせてシステムを実現する過程で，上述の機器レベルと同じ設計上の対処法も適用されますが，システム・レベルではシステム構築やシステム検証，運用手順の設定などの観点で信頼性を確保することに主眼が置かれます．例えば，フィールド・データの蓄積などは大きな財産になります．

参考・引用*文献

(1) 坂村健；ユビキタス，TRONに出会う ──「どこでもコンピュータ」の時代へ，NTT出版，2004年10月.
(2) Robert Baumann；“The Impact of Technology Scaling on Soft Error Rate Performance and Limits to the Efficacy of Error Correction”，IEDM 2002 IEEE，2002.

ひはら・ひろき
NEC東芝スペースシステム(株)